
Pliego técnico: Servicio de cifrado DRM

rtve

Índice	Página
1 Introducción.....	3
2 Descripción del servicio requerido.....	3
3 Requisitos técnicos del servicio.....	3
3.1 Servicios de cifrado requeridos.....	3
3.2 Licencias de visualización requeridas.....	4
3.3 Consumo de licencias.....	4
3.4 Compatibilidad con los reproductores existentes.....	5
3.5 Compatibilidad con herramientas de segmentación de vídeos.....	5
3.6 Compatibilidad con API de CRTVE.....	6
3.7 Compatibilidad con sistema de generación de tokens y cifrado.....	6
3.8 Claves de cifrado.....	6
3.9 Orígenes de vídeo VOD.....	7
3.10 Compatibilidad con vídeo en directo.....	7
3.11 Rendimiento de la solución.....	7
3.12 Capacidad del servicio y concurrencia de usuarios.....	7
3.13 Herramientas de gestión.....	7
3.14 Estadísticas y métricas.....	7
3.15 Documentación.....	8
3.16 Software como servicio.....	8
3.17 Soporte para integración y desarrollo.....	8
3.18 Evolución y mejora del servicio.....	8
4 Modelo de relación y seguimiento.....	8
4.1 Gestión de incidencias y soporte técnico.....	8
4.2 Evolución del servicio.....	9
4.3 Seguimiento de la prestación del servicio.....	9
5 Formato oferta.....	9

1 Introducción

CRTVE ofrece, a través de su página web www.rtve.es y aplicaciones para dispositivos conectados, diferentes tipos de contenidos informativos y de entretenimiento sobre los que posee derechos de emisión por Internet.

Sin embargo, no todos los programas para los que se tienen derechos de emisión por Internet se distribuyen actualmente a través de la web y aplicaciones de CRTVE, dado que es necesario hacer uso de tecnologías que impidan la redistribución y almacenamiento por terceros de los contenidos ofrecidos por CRTVE. El conjunto de tecnologías utilizadas para este fin recibe el nombre de DRM (Digital Rights Management).

Para asegurar la concurrencia de competidores, así como reducir los tiempos de migración entre proveedores DRM, la dirección de explotación y desarrollos interactivos de la CRTVE ha desarrollado un interfaz de aplicación (API) propio que garantiza la interoperabilidad de sus aplicaciones con múltiples proveedores de servicios DRM, siempre que estos cumplan con las especificaciones de este API.

2 Descripción del servicio requerido

Se requiere el servicio de protección de contenidos DRM que permita el cifrado de contenidos multimedia con DRM y proporcione licencias de reproducción de dicho contenido a los usuarios de la web y aplicaciones de CRTVE.

Este servicio debe ser compatible con las herramientas utilizadas por CRTVE para la generación de los flujos de vídeo bajo demanda (VOD) y directo (Live) en los formatos MPEG-DASH y HLS, así como con las aplicaciones de CRTVE para dispositivos conectados.

Además, el servicio de licencias DRM debe ser compatible con el API desarrollado por la dirección de explotación y desarrollos interactivos de la CRTVE que garantiza la interoperabilidad de sus aplicaciones con múltiples proveedores de servicios DRM.

3 Requisitos técnicos del servicio

3.1 Servicios de cifrado requeridos

Deben proporcionarse licencias, al menos, para las plataformas DRM que dan soporte a los navegadores y plataformas más utilizados por los usuarios de la web y aplicaciones de CRTVE:

- Apple Fairplay
- Google Widevine

Para reducir la complejidad de las tareas de cifrado de contenidos, también deberá permitir el uso de Common Encryption Scheme (CENC), incluyendo el esquema CBCS para su uso en contenidos protegidos con Fairplay.

Asimismo, el proveedor deberá proporcionar a CRTVE el software necesario para la obtención de las licencias correspondientes por parte de los usuarios, que se alojará en los servidores de CRTVE.

El número de licencias a consumir durante la prestación del servicio será de 250 millones (250.000.000).

3.2 Licencias de visualización requeridas

El servicio debe proporcionar diferentes tipos de licencias de uso de los elementos multimedia a los usuarios, en función de las posibilidades que ofrezca cada plataforma y los derechos de distribución con los que cuente CRTVE. Como mínimo deben ofrecerse este tipo de licencias para cada una de las tecnologías DRM requeridas:

- Licencias para reproducción online (con conexión a Internet), equivalentes a Fairplay Rental y Fairplay Lease.
- Licencias para reproducción offline (sin conexión a Internet), equivalentes a Fairplay persist.

Además, el servicio debe permitir la configuración de la licencia entregada al usuario en función de diferentes parámetros de configuración. Como mínimo debe permitirse esta configuración:

- Fecha de inicio de la licencia.
- Fecha de fin de la licencia.
- Tiempo máximo para reproducir el contenido desde el inicio de la reproducción.
- En el caso de licencias Widevine, además, debe permitirse la elección del nivel de seguridad (Widevine security level) asociado a la licencia. Debe permitirse elegir entre los niveles L1 y L3.

CRTVE podrá modificar el tipo y el tiempo de validez de las licencias entregadas en función del contenido entregado y el dispositivo sobre el que se reproducirá. El sistema ofrecido debe permitir la automatización de estas modificaciones mediante el uso de interfaces de aplicación (API) accesibles desde los centros de datos de CRTVE.

3.3 Consumo de licencias

Se considerarán como consumidas aquellas licencias entregadas por el licitador, según los siguientes casos de uso:

- Licencias expedidas para consumo de vídeo o audio bajo demanda online. Se considerará consumida una licencia por cada licencia diferente expedida a los usuarios de CRTVE para el consumo de un elemento cifrado con DRM.
- Licencias expedidas para consumo de vídeo o audio en directo. Se considerará consumida una licencia por la primera licencia expedida a un usuario durante la emisión de

un evento en directo. Así, un usuario que comience a ver un evento en directo sólo consumirá una licencia independientemente de la duración del mismo.

- Licencias expedidas para consumo de vídeo en directo offline. Se considerará consumida una licencia por la primera licencia expedida a un usuario para el consumo de un vídeo o audio durante el periodo de vigencia de la misma. Así, un usuario que obtenga una licencia para visualización de contenido offline, podrá reproducirlo tantas veces como determine CRTVE durante todo el periodo de vigencia de la licencia, y sólo se considerará como consumida una licencia.

3.4 Compatibilidad con los reproductores existentes

El software proporcionado tiene que incluir los SDK del servicio DRM para los siguientes entornos:

- Reproductor web basado en el proyecto VideoJS versión 7, con uso de las librerías contrib-hls y videojs-dash.
- Reproductor web basado en el proyecto Shaka Player.
- Reproductor nativo AVPlayer para aplicaciones móviles en entorno iOS.
- Reproductor ExoPlayer en aplicaciones móviles para sistema operativo Android.
- Dispositivos Google Chromecast.
- Dispositivos AppleTV.
- Dispositivos Amazon Fire TV.

Además, el licitador debe proporcionar las licencias de uso necesarias para los módulos software (SDK) requeridos para la visualización de contenidos cifrados con cualquiera de las tecnologías indicadas en el apartado 3.1 en aplicaciones nativas de los entornos indicados anteriormente.

3.5 Compatibilidad con herramientas de segmentación de vídeos

El software proporcionado debe ser compatible con las siguientes herramientas software utilizada por CRTVE para generación de vídeo protegido con DRM los vídeos en los formatos MPEG-DASH y HLS:

- Unified Origin – DRM del fabricante Unified Streaming, en versión 1.11.12 y superiores. Para todas las versiones, debe permitirse el uso de ficheros CPIX para el cifrado.
- Unified Packager – DRM del fabricante Unified Streaming, en versión 1.11.12 y superiores. Para todas las versiones, debe permitirse el uso de ficheros CPIX para el cifrado.
- Going del fabricante Golumi
- Golumito del fabricante Golumi

Asimismo, se requiere la posibilidad de desarrollar plugins para otras plataformas de codificación usadas por CRTVE.

3.6 Compatibilidad con API de CRTVE

El software proporcionado debe ser compatible con el API utilizado por las aplicaciones de CRTVE para la obtención de tokens de cifrado y reproducción.

La interfaz expuesta al usuario desde el servicio alojado en un dominio de CRTVE es la siguiente:

Método	URL	Respuesta en formato JSON
GET	/token/idasset	URL con licencia de reproducción Widevine URL con licencia de reproducción Fairplay URL de certificado Fairplay

Las URL con la licencia de reproducción se obtienen desde el servicio de obtención de tokens desarrollado por CRTVE de esta manera:

Se hace una única llamada HTTP al servicio del proveedor DRM por cada servicio DRM usado (Widevine y Fairplay) con la información relativa al asset a cifrar y la política de cifrado como un único parámetro de querystring en formato JWT (JSON Web Token) firmado con el algoritmo HS256 usando una clave privada compartida por el proveedor.

3.7 Compatibilidad con sistema de generación de tokens y cifrado

El software proporcionado tiene que ser compatible con los servicios de obtención de tokens, licencias de reproducción y certificados para contenidos protegidos por DRM desarrollados por CRTVE descritos en el apartado 3.6.

Igualmente, tiene que ser compatible con el servicio de obtención de ficheros CPIX desarrollado por CRTVE para su uso por parte del software del fabricante Unified Streaming indicado en el apartado 3.5.

Por último, el software proporcionado tiene que permitir el acceso a los servicios de emisión de licencias y cifrado de contenidos a través de subdominios de rtve.es mediante el uso de un proxy o aplicación intermedia alojada bajo un subdominio de rtve.es.

De este modo, las aplicaciones de CRTVE no deberán modificarse de forma sustancial en caso de cambio del proveedor de servicios DRM.

3.8 Claves de cifrado

El servicio debe permitir a CRTVE la obtención de las claves de cifrado y su almacenamiento para uso posterior con otros proveedores de servicios DRM.

3.9 Orígenes de vídeo VOD

La solución presentada para los vídeos VOD debe permitir el cifrado de los vídeos en el momento de ser servidos al usuario (cifrado al vuelo), utilizando los vídeos existentes en los sistemas indicados por CRTVE, así como el cifrado offline para su posterior almacenamiento y distribución.

3.10 Compatibilidad con vídeo en directo

La solución presentada debe ser compatible con el cifrado y reproducción de eventos en directo, utilizando software de codificación compatible.

3.11 Rendimiento de la solución

Se requieren unas características de rendimiento a las soluciones presentadas, que garanticen que cumplen con las expectativas de RTVE para este servicio. Así, el servicio debe proporcionarse a través de una arquitectura autoescalable que se adapte al número de usuarios concurrentes que haya en cada momento.

Debe permitir la solicitud y entrega de hasta 1.000 licencias por segundo. Para asegurar el correcto funcionamiento del servicio, se requiere además la posibilidad de reservar capacidad garantizada adicional durante 24 horas en bloques de 100 licencias de emisión por segundo, hasta un máximo de 2.000. peticiones por segundo.

Se valorarán positivamente aquellas propuestas que permitan la emisión de más de 3.000 licencias por segundo en picos de consumo.

3.12 Capacidad del servicio y concurrencia de usuarios

Cualquier solución presentada debe permitir el acceso simultáneo de 1.500.000 usuarios simultáneos, con hasta un millón y medio (1.500.000) de peticiones diarias para todos los vídeos.

3.13 Herramientas de gestión

El servicio deberá incluir herramientas de gestión del mismo, a modo de panel de control, accesibles a través de Internet mediante un navegador web.

Estas herramientas deben permitir, como mínimo:

- Consultar las estadísticas y métricas recopiladas por el servicio.

3.14 Estadísticas y métricas

Deben proporcionarse estadísticas de uso y métricas del servicio que permitan identificar claramente el número de licencias entregadas. Además, debe cumplir con los siguientes requisitos:

- El servicio de métricas debe proporcionarse a través de una web accesible a cualquier hora, todos los días del año.

- Asimismo, debe permitir obtener información sobre el número y tipo de licencias entregadas de forma mensual y diaria.

3.15 Documentación

El proveedor debe proporcionar la documentación necesaria para el desarrollo de un software que permita generar URL de reproducción válidas a partir de un identificador único formado por caracteres alfanuméricos, con diferentes tipos de licencia y solución DRM. Esta documentación debe estar accesible a través de Internet o enviarse por correo electrónico bajo petición de CRTVE.

3.16 Software como servicio

CRTVE no alojará ningún software en sus equipos ni en los centros de datos que CRTVE utiliza para albergar sus propios servidores, excepto el API descrito en el apartado 3.7..

3.17 Soporte para integración y desarrollo

El licitador deberá proporcionar la información necesaria para la integración de aplicaciones propias de CRTVE o de terceros autorizados por ella, con el fin de que se integren con el servicio de cifrado DRM proporcionado.

3.18 Evolución y mejora del servicio

El adjudicatario proporcionará sin coste adicional aquellas actualizaciones del software que redunden en una mejora del servicio ofrecido a los usuarios, o en la reducción de uso de elementos de cómputo por parte de CRTVE.

4 Modelo de relación y seguimiento

El modelo de relación que se establecerá entre CRTVE y el adjudicatario tiene como objetivo garantizar el control y el seguimiento del servicio que se tiene que proveer. También tiene como misión la trazabilidad y la supervisión de los proyectos que dicho servicio ejecutará.

Se requiere la asignación de un Technical Account Manager (TAM) que asistirá a CRTVE durante las fases de implantación del servicio, así como durante el resto del tiempo del contrato para la operación del servicio. Este interlocutor técnico se responsabilizará de asegurar la mejora continua del servicio, así como de gestionar o escalar las peticiones más urgentes y las incidencias más graves.

4.1 Gestión de incidencias y soporte técnico

El adjudicatario deberá ofrecer soporte técnico en castellano o inglés tanto por teléfono con numeración española, correo electrónico y mediante un sistema automatizado de

gestión de tickets. El horario de atención de soporte de ser, como mínimo, de lunes a viernes de 9:00 a 18:00 (hora peninsular española).

También debe proporcionarse un canal de soporte 24x7 a través de Internet (mediante chat o teleconferencia) para la notificación de incidencias urgentes o peticiones de soporte. Este soporte 24x7 se podrá proporcionar en castellano o en inglés.

4.2 Evolución del servicio

El adjudicatario, a través del TAM, notificará las actualizaciones disponibles en el servicio y evaluará las peticiones de CRTVE para la mejora del mismo.

4.3 Seguimiento de la prestación del servicio

El seguimiento del servicio se hará de manera periódica y continuada, para evaluar el rendimiento del servicio y la evolución tecnológica del mismo. Las reuniones se realizarán de manera telemática.

5 Formato oferta

Al margen de lo que se mencione en los adjuntos a este documento, las ofertas deben contener:

- Resumen ejecutivo (máximo 5 páginas):
 - Debe describir la oferta técnica, en resumen.
- Documento de ajuste a requisitos:
 - Se enumerarán con detalle técnico todas las características técnicas de la solución propuesta.